## RESPONSE
## Remarks

Claims 1-16 are pending in the application. Claims 1, 6 and 13 are in independent format. The claims have been amended to further clarify features of the Applicant's invention.

The Applicant traverses all the Examiner's rejections and assertions. The Applicant may respond only to specific assertions by the Examiner but intends to traverse all rejections and assertions made by the Examiner.

## TELEPHONE INTERVIEW WITH THE EXAMINER

## ON February 11, 2009

The Applicant thanks the Examiner for his insight and courtesy during the telephone interview with the Examiner on February 11, 2009. The Applicant's amendment and response are based on the interview and the understandings gained therein.

## Information Disclosure Statement Comment

The Examiner asserted "The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered."

## Information Disclosure Statement Response

The Applicant traverses all the Examiner's rejections and assertions. The Applicant may respond only to specific assertions by the Examiner but intends to traverse all rejections and assertions made by the Examiner.

The Applicant submit an Information Disclosure Statement on January 22, 2008. The Applicant acknowledges that the Examiner has considered all of the cited references on this Supplemental IDS and publication dates cited thereon.

## Section 101 Rejection

The Examiner asserts "Claims 1, 6 and 13 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. Supreme Court precedent' and recent Federal Circuit decisions2 indicate that a statutory "process" under 35 U.S.C. 101 must (1) be tied to another statutory category (such as a particular apparatus), or (2) transform underlying subject matter (such as an article or material) to a different state or thing. While the instant claim(s) recite a series of steps or acts to be performed, the claim(s) neither transform underlying subject matter nor positively tie to another statutory category that accomplishes the claimed method steps, and therefore do not qualify as a statutory process. For example, claim 1 discloses "obtaining a user biometric from a biometric system" and "storing the dependency vector in an Identification and Verification Template (IVT) on a reliable storage medium" which are directed to insignificant pre and post processing and do not satisfy the requirement of being tied to another statutory category."

## Section 101 Response

The Applicant traverses all the Examiner's rejections and assertions. The Applicant may respond only to specific assertions by the Examiner but intends to traverse all rejections and assertions made by the Examiner.

The Applicant has amended the independent claims based on the understanding gained with the Examiner during the phone interview. The applicant submits that the claims as amended, which include references to servers and information bits, are now statutory and the requests the Section 101 rejection be immediately withdrawn.

## Section 102 Rejection

The Examiner asserts "Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by the article "On Enabling Secure Applications Through Off-line Biometric Identification" to Davida et al. ("Davida") (already of record)."

## Section 102 Response

The Applicant traverses all the Examiner's rejections and assertions. The Applicant may respond only to specific assertions by the Examiner but intends to traverse all rejections and assertions made by the Examiner.

The reference cited by the Examiner will be called the "Davida paper" hereinafter to avoid confusion. The current Applicant is Dr. George Davida, the author of the Davida paper cited by the Examiner.

### 1. THE DAVIDA PAPER IS NOT A VALID 102(b) REFERENCE

First, the Applicant submits that the Davida reference cannot anticipate the Applicant's invention under §102(b). 35 U.S.C. §102(b) recites "A person shall be entitled to a patent unless the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States."

The Davida paper cited by the Examiner, according to the IEEE, was officially published by the IEEE in the *Proceedings of Security and Privacy Symposium* held in Oakland, California on May 3 through May 6, 1998. The current Application was filed on April 30, 1999. Assuming the earliest publication date of May 3, 1998, the current application was filed less than one year after the publication of the Davida paper. Within the one year time frame required by §102(b).

Tables 1 and 2 illustrate the official electronic IEEE publication entries for the Davida paper obtained from the Internet. The Applicant includes the URL's used to obtain the information for the Examiner's convenience. The Applicant also includes a printed copy from the IEEE web-site printouts in Exhibits A and B. The Examiner can use the same URL's to verify the entries included.

URL: http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=674831

**On enabling secure applications through off-line biometric identification**
Davida, G.I.; Frankel, Y.; Matt, B.J.;
Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on
3-6 May 1998 Page(s):148 - 157
**Abstract:**

In developing secure applications and systems, designers must often incorporate secure user identification in the design specification. In this paper, we study secure off-line authenticated user identification schemes based on a biometric system that can measure a user's biometrics accurately (up to some Hamming distance). The presented schemes enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as a magnetic strip. Also developed are schemes specifically designed to minimize the compromising of a user's private biometrics data, encapsulated in the authorization information, without requiring secure hardware tokens. We also study the feasibility of biometrics performing as an enabling technology for secure systems and applications design. We investigate a new technology which allows a user's biometrics to facilitate cryptographic mechanisms

Table 1.

URL--
http://ieeexplore.ieee.org/search/freesrchabstract.jsp?arnumber=674831&isnumber=14832&punumber=5528&k2dockey=674831@ieeecnfs&query=674831%3Cin%3Earnumber&pos=0

On enabling secure applications through off-line biometric identification

Davida, G.I.   Frankel, Y.   Matt, B.J.
Wisconsin Univ., Milwaukee, WI, USA ;
This paper appears in: Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on
Publication Date: 3-6 May 1998
On page(s): 148 - 157
Number of Pages: ix+225
Meeting Date: 05/03/1998 - 05/06/1998
Location: Oakland, CA
ISBN: 0-8186-8386-4
Digital Object Identifier: 10.1109/SECPRI.1998.674831
Current Version Published: 2002-08-06

Table 2.

The Applicant calls the Examiner's attention to the ISBN number in Table 2. The ISBN number for the publication is listed as 0-8186-8386-4. On the Davida paper in the lower right hand corner, this ISBN number is included in a string of text listed as "0-8186-8386-4/98 $10.00 © 1998 IEEE." See Exhibit C. This is the same ISBN number with an additional slash "/" character and the number "98."

The original Examiner on this matter, Examiner Vikkram Bali, apparently incorrectly assumed that the publication of the Davida paper was from April of 1998 because of the reference to "4/98" in the information on the paper. However, the 4/98 is not for April 1998, but instead is the last digit of the ISBN number, namely, 4, and the year of publication 1998. Without closer examination, the Examiner apparently just assumed the Davida paper was published in April of 1998. See Box, U, paper 4, in the *Notices of References Cited*, paper dated 11-29-2001, included as Exhibit D. There is no specific date in Box U for the Davida paper, only April, 1998.

However, if the current Examiner will examine the Davida paper and the ISBN number listed in Table 2 for the IEEE publication entry, he will see that Examiner Bali may have incorrectly assumed that the paper was published in April of 1998, when it was actually published at the earliest, on May 3, 1998, three days after the Applicant filed the current application. Thus, the Applicant filed the current application at least three days before the one year deadline requirement of §102(b). The Applicant correctly noted the publication date of the Davida paper on the IDS filed by Applicant on January 22, 2008, and considered by the current Examiner.

The Applicant submits the Davida paper is not a proper §102(b) reference at all because the Applicant filed the current application three days before the one year deadline required by §102(b). However, should the Examiner disagree, the Applicant very respectfully asks the Examiner to submit proof in writing of an actual earlier publication date of the Davida paper than that of May 3, 1998 as indicated by the IEEE.

## <u>2. NOT ALL OF THE CLAIM ELEMENTS ARE DESCRIBED BY THE DAVIDA PAPER</u>

Even if the Davida paper is a valid 102(b) reference, and the Applicant respectfully submits that is not, the Examiner is reminded that a claim is anticipated under 35 U.S.C. §102 <u>only if each and every element as set forth in the</u>

claim is found either, expressly or inherently described, in a single prior art reference. *Vergegall Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987).

The Examiner is also reminded that to maintain a *prima case* of anticipation, the identical invention must shown in as complete detail in a single prior art reference as is contained in the anticipated claim. *Richardson v. Suzuki Motor Co.,* 868 F.2d 1226, 1236 (Fed. Cir. 1989).

All of the independent claims include claim elements, including but not limited to: *creating an Identification and Verification Template from a biometric collected from a user with a lossy transformation of information from the user biometric.*

The Davida reference, written by the same Applicant as the current Applicant, does not include the words "*lossy transformation*" at all. Thus, the Davida paper cannot expressly described claimed invention and does not described the claimed invention in complete detail since it does not include the words "*lossy transformation*" anywhere at all.

Therefore, the §102(b) rejection of claims 1-16 is clearly improper and must be immediately withdrawn. The Applicant requests claims 1-16 be immediately passed to publication.

## CONCLUSION

None of the prior art made of record in the Office Action but not relied upon by the Examiner is any more pertinent to Applicant's invention than the cited references for the reasons given above. The Applicant therefore submits that all of the claims in their present form are immediately allowable and requests the Examiner withdraw the §101 and §102 rejections of all the claims and pass all of the pending claims 1-16 to allowance.

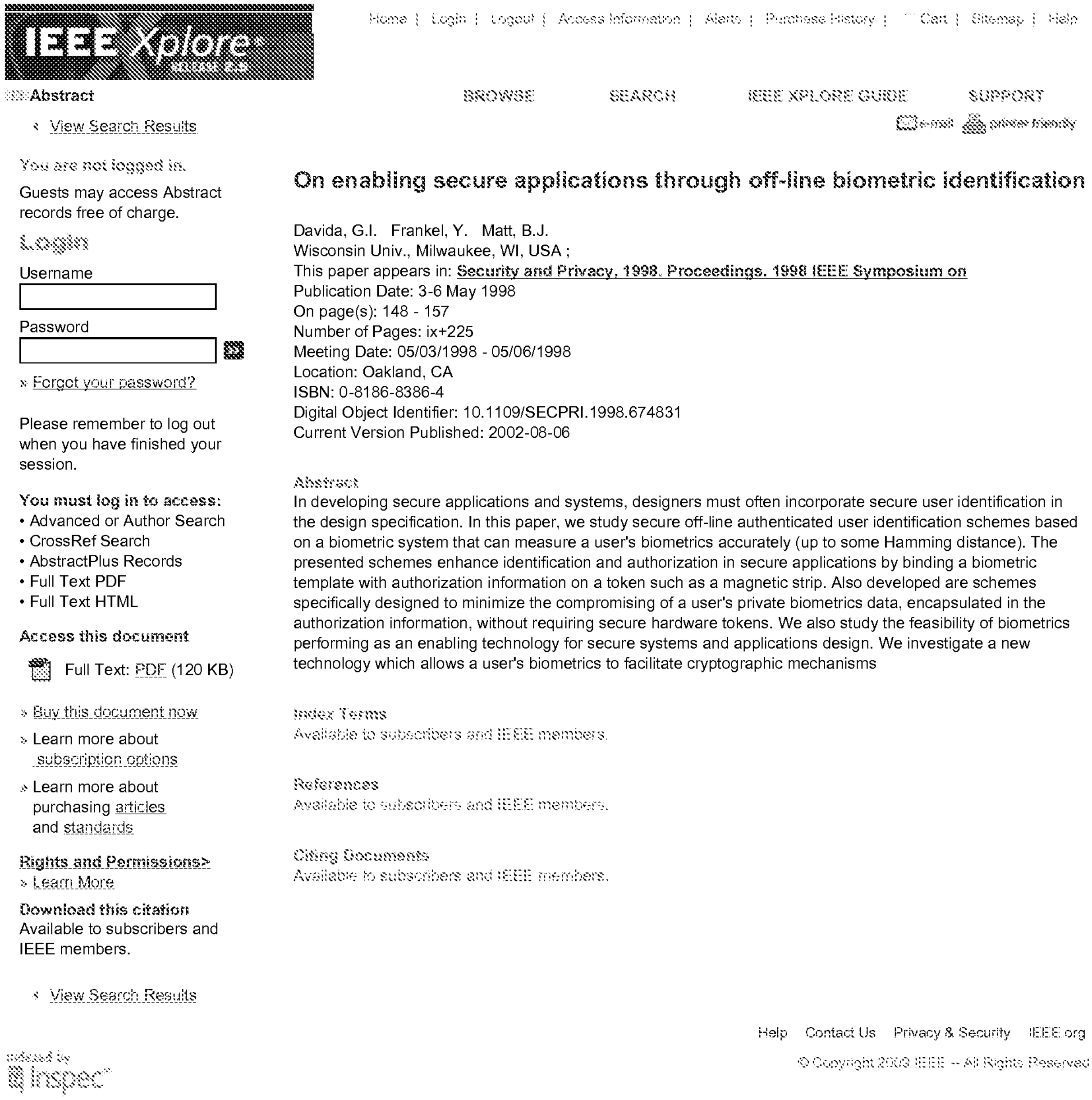
Respectfully submitted,

**Lesavich High-Tech Law Group, P.C.**

Date: February 13, 2009

By: Stephen Lesavich
Stephen Lesavich
Registration No. 43,749

EXHIBIT A



Abstract

‹ View Search Results

You are not logged in.

Guests may access Abstract records free of charge.

Login

Username

Password

» Forgot your password?

Please remember to log out when you have finished your session.

**You must log in to access:**
- Advanced or Author Search
- CrossRef Search
- AbstractPlus Records
- Full Text PDF
- Full Text HTML

**Access this document**

Full Text: PDF (120 KB)

» Buy this document now

» Learn more about subscription options

» Learn more about purchasing articles and standards

**Rights and Permissions>**

» Learn More

**Download this citation**

Available to subscribers and IEEE members.

‹ View Search Results

## On enabling secure applications through off-line biometric identification

Davida, G.I. Frankel, Y. Matt, B.J.
Wisconsin Univ., Milwaukee, WI, USA ;

This paper appears in: Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on
Publication Date: 3-6 May 1998
On page(s): 148 - 157
Number of Pages: ix+225
Meeting Date: 05/03/1998 - 05/06/1998
Location: Oakland, CA
ISBN: 0-8186-8386-4
Digital Object Identifier: 10.1109/SECPRI.1998.674831
Current Version Published: 2002-08-06

Abstract

In developing secure applications and systems, designers must often incorporate secure user identification in the design specification. In this paper, we study secure off-line authenticated user identification schemes based on a biometric system that can measure a user's biometrics accurately (up to some Hamming distance). The presented schemes enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as a magnetic strip. Also developed are schemes specifically designed to minimize the compromising of a user's private biometrics data, encapsulated in the authorization information, without requiring secure hardware tokens. We also study the feasibility of biometrics performing as an enabling technology for secure systems and applications design. We investigate a new technology which allows a user's biometrics to facilitate cryptographic mechanisms

Index Terms
Available to subscribers and IEEE members.

References
Available to subscribers and IEEE members.

Citing Documents
Available to subscribers and IEEE members.

Help Contact Us Privacy & Security IEEE.org

EXHIBIT B

IEEE Xplore RELEASE 2.5

Home | Login | Logout | Access Information | Alerts | Purchase History | Cart | Sitemap | Help

CrossRef Search

BROWSE SEARCH IEEE XPLORE GUIDE SUPPORT

**You requested this document:**

» Key

| | |
|---|---|
| IEEE JNL | IEEE Journal or Magazine |
| IEE JNL | IEE Journal or Magazine |
| IEEE CNF | IEEE Conference Proceeding |
| IEE CNF | IEE Conference Proceeding |
| IEEE STD | IEEE Standard |

1. **On enabling secure applications through off-line biometric identification**
Davida, G.I.; Frankel, Y.; Matt, B.J.;
Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on
3-6 May 1998 Page(s):148 - 157
**Abstract:**

In developing secure applications and systems, designers must often incorporate secure user identification in the design specification. In this paper, we study secure off-line authenticated user identification schemes based on a biometric system that can measure a user's biometrics accurately (up to some Hamming distance). The presented schemes enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as a magnetic strip. Also developed are schemes specifically designed to minimize the compromising of a user's private biometrics data, encapsulated in the authorization information, without requiring secure hardware tokens. We also study the feasibility of biometrics performing as an enabling technology for secure systems and applications design. We investigate a new technology which allows a user's biometrics to facilitate cryptographic mechanisms

Abstract | Full Text: PDF(120 KB) IEEE CNF

Help Contact Us Privacy & Security IEEE.org

EXHIBIT C

| | | |
|---|---|---|
| ***Notice of References Cited*** | Application/Control No.<br>09/303,053 | Applicant(s)/Patent Under Reexamination<br>DAVIDA ET AL. |
| | Examiner<br>Vikkram Bali | Art Unit<br>2623 \| Page 1 of 1 |

## U.S. PATENT DOCUMENTS

| * | | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name | Classification | |
|---|---|---|---|---|---|---|
| | A | US-6038315 | 03-2000 | Strait et al | 380 | 23 |
| | B | US-4993068 | 02-1991 | Piosenka et al | 235 | 380 |
| | C | US-6309069 B1 | 10-2001 | Steal et al | 351 | 221 |
| | D | US-5434917 | 07-1995 | Naccache et al | 380 | 23 |
| | E | US- | | | | |
| | F | US- | | | | |
| | G | US- | | | | |
| | H | US- | | | | |
| | I | US- | | | | |
| | J | US- | | | | |
| | K | US- | | | | |
| | L | US- | | | | |
| | M | US- | | | | |

## FOREIGN PATENT DOCUMENTS

| * | | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification | |
|---|---|---|---|---|---|---|---|
| | N | | | | | | |
| | O | | | | | | |
| | P | | | | | | |
| | Q | | | | | | |
| | R | | | | | | |
| | S | | | | | | |
| | T | | | | | | |

## NON-PATENT DOCUMENTS

| * | | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|---|
| | U | IEEE Security and Privacy proceedings, April 1998, On Enabling Secure Applications Through Off-line Biometric Identification, by Davida et al., pages 148-157 |
| | V | |
| | W | |
| | X | |

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EXHIBIT D

# On Enabling Secure Applications Through Off-line Biometric Identification

George I. Davida
Univ. of Wisconsin-Milwaukee
Milwaukee, WI
davida@cs.uwm.edu

Yair Frankel
CertCo LLC
New York, NY
yfrankel@cs.columbia.edu

Brian J. Matt
Sandia National Laboratories*
Albuquerque, NM
bjmatt@cs.sandia.gov

**Abstract**

*In developing secure applications and systems, the designers often must incorporate secure user identification in the design specification. In this paper, we study secure off-line authenticated user identification schemes based on a biometric system that can measure a user's biometric accurately (up to some Hamming distance). The schemes presented here enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as a magnetic strip. Also developed here are schemes specifically designed to minimize the compromise of a user's private biometrics data, encapsulated in the authorization information, without requiring secure hardware tokens.*

*In this paper we furthermore study the feasibility of biometrics performing as an enabling technology for secure system and application design. We investigate a new technology which allows a user's biometrics to facilitate cryptographic mechanisms.*

## 1 Introduction

Secure digital identification schemes are becoming increasingly important, as more security applications require identification based on physical characteristics rather than solely on a user's knowledge of a secret cryptographic key or password. The increased interest in such applications, ranging from door access to electronic commerce applications, has led to an increased interest in methods for secure and accurate identification [8, 5, 18, 17] of individuals as well as machines and objects. In this paper we are interested in systems of identification that use measurable biological features, biometrics, which can be readily measured at the point of application. It is desirable that such measurements be non-invasive and simple to perform. One biometric that has been suggested is the iris scan [3, 12, 6, 21].

On-line applications secured through the use of biometric authentication typically are based on a push or pull model. In both models, the first step is a user initialization, which occurs when the user's biometric template is registered with the on-line server. After initialization, when a user wants access that requires biometric identification, a *biometric authorization process* is performed. At this time the user's biometric is read by a reader. In the push model, the reader transmits (preferably via a private channel) the reading to the on-line server; the on-line server then verifies the validity of the reading based on the user's template in the server's directory; and finally the server sends an authenticated acceptance or rejection message back to the reader. In the pull model, the reader requests the template from the server, and the reader performs the verification steps after receiving the template over an authenticated and, preferably, private channel from the server. In both cases, an authenticated channel is necessary for some communications between the on-line database and the reader. The authentication can also provide for a binding of a user's biometric with some form of authorization, as established by trust relationships between the reader and the on-line database.

Here we are interested in developing biometric based identification systems which do not require the incorporation of an on-line database for the security infrastructure. Such databases are not always practical in mobile environments, such as military applications, and are often cost prohibitive since they require expensive wiring for connectivity or costly wireless devices. In order to remove the connectivity requirements, an *off-line* biometric system is achieved by incorporating a biometric template on a storage device / token (e.g., magnetic strip or smartcard) which provides for a reliable storage medium; however, there are no security requirements required of the token. We, therefore, will work in the pull model with the storage device containing sufficient information to validate the authenticity of the user's acquired biometric template to the biometric generated during user initialization. To provide for the user biometric/user authorization binding, a trusted authorization officer who authenticates (signs) the user's biometric template is incorporated into our infrastructure.

A biometric identification system which provides

[*] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

0-8186-8386-4/98 $10.00 © 1998 IEEE